



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/707,417	11/06/2000	Vance C. Bjorn	003022.P019X	9958

7590

11/14/2005

Judith A. Szepesi  
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP  
Seventh Floor  
12400 Wilshire Boulevard  
Los Angeles, CA 90025-1026

EXAMINER

MOORTHY, ARAVIND K

ART UNIT

PAPER NUMBER

2131

DATE MAILED: 11/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No. 09/707,417	Applicant(s) BJORN, VANCE C.	
	Examiner Aravind K. Moorthy	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 25 August 2005.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-31 is/are pending in the application.  
     4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-31 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 November 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
     a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. This is in response to the amendment filed on 25 August 2005.
2. Claims 1-31 are pending in the application.
3. Claims 1-31 have been rejected.

### ***Response to Arguments***

4. Applicant's arguments with respect to claims 1-31 have been considered but are moot in view of the new ground(s) of rejection.

### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 1-31 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

As to claim 1, the limitation of “the record ID being a random record ID generated for tracking authentication data” is not enabled by the specification.

As to claim 14, the limitation of “the random record ID used to separate the user's identity from authentication data” is not enabled by the specification.

As to claim 17, the limitation of “the record ID randomly generated to separate the user's identity from authentication data” is not enabled by the specification.

Any claims not directly addressed are rejected on the virtue of their dependency.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**6. Claims 1-6, 8, 9, 11-14, 17, 20-24, 26, 27 and 29-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dickinson et al U.S. Patent No. 6,853,988 B1 in view of Nguyen et al U.S. Patent No. 6,006,334.**

As to claims 1, 2 and 20, Dickinson et al discloses a method of authenticating a client, the method comprising:

a one-time key generated by the server and encrypted with a user's public key by the server [column 28 line 66 to column 29 line 27];

receiving the user's authentication data from the client [column 29, lines 28-38];

determining if the user's authentication data matches the record ID [column 29, lines 28-38]; and

if so, decrypting the one-time key with the user's private key, and returning the decrypted one-time key to the client [column 29, lines 39-51];

generating a random public key/private key pair for the user [column 7, lines 53-65].

Dickinson et al does not teach generating the random record ID for the user. Dickinson et al does not teach associating the authentication data and the private key with the record ID.

Art Unit: 2131

Dickinson et al does not teach the record ID being a random record ID generated for tracking authentication data.

Nguyen et al teaches generating a random record ID for the user [column 4 line 64 to column 5 line 23]. Nguyen et al teaches the random record ID generated for tracking authentication data [column 4 line 64 to column 5 line 23].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dickinson et al so that a random record ID would have been generated for a user. The random record ID would have been used for tracking the authentication data.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dickinson et al by the teaching of Nguyen et al because the random factor helps recognize compromised passwords [column 1, lines 59-62].

As to claims 3 and 21, Dickinson et al teaches sending the record ID and the public key to the user [column 11, lines 28-35].

As to claims 4 and 22, Dickinson et al teaches establishing a secure connection with the user, prior to receiving registration authentication data [column 6, lines 13-29].

As to claims 5 and 23, Dickinson et al teaches a web page presented by the server to the client prompts the user to enter the authentication data to log in to the server [column 14, lines 16-21].

As to claims 6 and 24, Dickinson et al teaches that the client's authentication data is automatically redirected to the authentication server [column 14, lines 34-57].

As to claims 8 and 26, Dickinson et al teaches that the authentication data is personal data selected from among the following: a password, a smart card, and another type of authentication card [column 12, lines 21-32].

As to claims 9 and 27, Dickinson et al teaches that the client forwards the decrypted one-time key to the server, thereby authenticating the user as the owner of the private key [column 7, lines 53-65].

As to claims 11 and 29, Dickinson et al teaches that the record ID and the encrypted one-time key are further encrypted using a partner key. Dickinson et al teaches decrypting the record ID and encrypted one-time key using the partner key [column 48 line 62 to column 49 line 13].

As to claims 12 and 30, Dickinson et al teaches that the partner key is a symmetric key set up during registration of the partner [column 8, lines 7-14].

As to claims 13 and 31, Dickinson et al teaches that the partner key is a private key of the authentication server [column 8, lines 7-14].

As to claim 14, Dickinson et al discloses a method of using an authentication server to authenticate a user to a third party server, the method comprising the third party server:

generating a one-time key and encrypting the one-time key with a public key of the user, and sending the encrypted one-time key and the record ID to the user;

receiving the authentication data, the authentication data being the decrypted one-time key decrypted with the user's private key by the

Art Unit: 2131

authentication server, such that the user does not have control of the user's private key at any time; and

permitting access to the server.

Dickinson et al does not teach looking up a random record ID associated with the user. Dickinson et al does not teach the random record ID used to separate the user's identity from authentication data.

Nguyen et al teaches looking up a random record ID associated with the user [column 4 line 64 to column 5 line 23]. Nguyen et al teaches the random record ID used to separate the user's identity from authentication data [column 4 line 64 to column 5 line 23].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dickinson et al so that there would have been a random record ID generated that would have been associated with the user. The random record ID would have been used to separate the user's identity from the authentication data.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dickinson et al by the teaching of Nguyen et al because the random factor helps recognize compromised passwords [column 1, lines 59-62].

As to claim 17, Dickinson et al discloses a third-party authentication system comprising:

a one-time key generated by a third party server and encrypted with a user's public key by the third party server, as discussed above;

a comparison logic in the authentication server to receive the user authentication data from the client and determine whether the user's authentication data matches the record ID, as discussed above; and

a decryption logic in the authentication server to decrypt the one-time key with a private key associated with the validated record ID, and to return the decrypted one-time key to the client, as discussed above.

Dickinson et al does not teach looking up a random record ID associated with the user. Dickinson et al does not teach the random record ID used to separate the user's identity from authentication data.

Nguyen et al teaches looking up a random record ID associated with the user [column 4 line 64 to column 5 line 23]. Nguyen et al teaches the random record ID used to separate the user's identity from authentication data [column 4 line 64 to column 5 line 23].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dickinson et al so that there would have been a random record ID generated that would have been associated with the user. The random record ID would have been used to separate the user's identity from the authentication data.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dickinson et al by the teaching of Nguyen et al because the random factor helps recognize compromised passwords [column 1, lines 59-62].

**7. Claims 7, 10, 25 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dickinson et al U.S. Patent No. 6,853,988 B1 and Nguyen et al U.S. Patent No. 6,006,334 as applied to claim 1 above, and further in view of Byford U.S. Patent No. 6,581,161 B1.**

As to claims 7, 10, 25 and 18, the Dickinson-Nguyen combination teaches that the authentication data is biometric data [Dickinson et al figure 1].



The Dickinson-Nguyen combination does not teach discarding the record ID after returning the one-time key to the user.

Byford teaches authentication data being biometric data [column 4 lines 44-58]. Byford teaches discarding a user's record ID [column 2, lines 39-42].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Dickinson-Nguyen combination so that the authentication data was biometric data and the user's record ID would have been discarded.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Dickinson-Nguyen combination by the teaching of Byford because it removes the need for encoded badges, static passwords and the like, and also removes the need for users to present themselves at a particular location, such as a security control office, before they can be granted access rights to a facility [column 4, lines 59-67].

**8. Claims 15, 16, 18 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dickinson et al U.S. Patent No. 6,853,988 B1 and Nguyen et al U.S. Patent No. 6,006,334 as applied to claims 14 and 17 above, and further in view of Towers et al U.S. Patent No. 5,692,106.**

As to claims 15, 16 and 18, the Dickinson-Nguyen combination does not teach determining an authentication policy associated with the user. The Dickinson-Nguyen combination does not teach verifying that the authentication policy has been satisfied, prior to permitting access to the server. The Dickinson-Nguyen combination does not teach determining if the server should verify additional data. The Dickinson-Nguyen combination does not teach requesting additional data from the user prior to generating the onetime key.

Art Unit: 2131

Towers et al teaches determining an authentication policy associated with the user [column 13, lines 31-48]. Towers et al teaches verifying that the authentication policy has been satisfied, prior to permitting access to the server [column 13, lines 31-48]. Towers et al teaches determining if the server should verify additional data [column 1, lines 36-63]. Towers et al teaches requesting additional data from the user prior to generating the one-time key [column 1, lines 36-63].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Dickinson-Nguyen combination so that an authentication policy associated with the user was verified prior to permitting access to the server. Should additional user information was needed; it would have been requested prior to generating the one-time key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Dickinson-Nguyen combination by the teaching of Towers et al because the examiner asserts that authentication policies restrict what a user can do on a server site and requesting additional data further authenticates a user prior to accessing a server's site.

As to claim 21, the Dickinson-Nguyen combination teaches that the interface sends the record ID and the public key to the user, as discussed above.

Art Unit: 2131

**9. Claims 19 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dickinson et al U.S. Patent No. 6,853,988 B1 and Nguyen et al U.S. Patent No. 6,006,334 as applied to claim 17 above, and further in view of Mao U.S. Patent No. 6,119,227.**

As to claim 19, the Dickinson-Nguyen combination does not teach nonce generation logic to generate a nonce. The Dickinson-Nguyen combination does not teach that the nonce is to be included with the user authentication data from the client. The Dickinson-Nguyen combination does not teach comparison logic to verify that the user authentication data includes the appropriate nonce.

Mao teaches nonce generation logic to generate a nonce [column 5, lines 13-29]. Mao teaches that the nonce is to be included with the user authentication data from the client [column 5, lines 30-51]. Mao teaches comparison logic to verify that the user authentication data includes the appropriate nonce [column 5, lines 30-51].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Dickinson-Nguyen combination so that there was nonce generation logic to generate a nonce. The nonce is would have been included with the user authentication data from the client. Comparison logic would have been used to verify that the user authentication data includes the appropriate nonce.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Dickinson-Nguyen combination by the teaching of Mao because it provides a method for authenticating a user's requests and messages [column 1, lines 49-67]

Art Unit: 2131

As to claim 22, the Dickinson-Nguyen combination teaches that interface establish a secure connection with the user, prior to receiving registration authentication data, as discussed above.

***Conclusion***

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

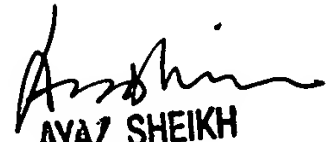
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy   
November 8, 2005

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100